OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

February 21, 2001

MEMORANDUM FOR CHIEF INFORMATION OFFICER, DEPARTMENT OF THE ARMY
CHIEF INFORMATION OFFICER, DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER, DEPARTMENT OF THE AIR FORCE
CHIEF INFORMATION OFFICERS, DEFENSE AGENCIES
DIRECTOR OF JOINT STAFF
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS
AND COMPUTERS, JOINT STAFF (J-6)

SUBJECT: DoD Information Technology (IT) Registry

Section 8102(a) of the FY 2001 National Defense Appropriation Act and Section 811(a) of the FY 2001 National Defense Authorization Act states that no funds appropriated in FY 2001 may be used and prohibits awarding contracts for mission critical (MC)/mission essential (ME) IT systems unless they are registered with the DoD CIO. The Secretary of Defense must report to Congress on the status of Section 811(a) implementation on April 1 for the next three years starting in 2001. We will continue to use the DoD IT Registry as the system of record to maintain system registration to comply with congressional requirements and to serve as a technical repository to support CIO assessments.

As with last year's registration, CINC/Service/Agency CIOs will certify to the DoD CIO, by letter, all MC/ME IT systems have been registered by March 22, 2001. The attached DoD IT Registry Implementation Instructions provide additional details for updating this key registry. My POC for the DoD IT Registry is Mr. Gary Evans @ (703) 602-0980 x137 or gary.evans@osd.mil.

In a manner prescribed by their respective CIOs, each CINC/Service/Agency will maintain interface data and contingency plans for each registered MC/ME IT system. Additional information on next year's certification requirements for interfaces and contingency plans will be provided at a later date.

Paul R. Brubaker
Deputy Assistant Secretary of Defense
(Deputy CIO)

Attachment:
As Stated

DoD IT REGISTRY
IMPLEMENTING INSTRUCTIONS

SUBJECT: DoD IT Registry Implementing Instructions

Section 8102(a) of the FY 2001 National Defense Appropriation Act and Section 811(a) of the FY 2001 National Defense Authorization Act require that:

- Each DoD MC/ME IT system be registered with the DoD CIO,
- A consolidated inventory of those systems be maintained,
- Interfaces between those systems and other systems must be identified, and
- Contingency plans must be developed and maintained.

What must be Registered

The referenced legislation states that unless registered: funds appropriated in FY 2001 may not be used for MC/ME IT systems, and prohibits DoD from awarding contracts for MC/ME IT systems, or approving milestones for Major Automated Information Systems (MAIS). The Secretary of Defense must report to Congress on the status of Section 811(a) implementation on April 1, 2001, 2002, and 2003.

The DoD IT Registry must contain all MC/ME IT systems that are fielded, as well as all the MC/ME IT systems in development, i.e., all Acquisition Category I through IV programs.

An information system is defined in Section 3502(8), Title 44, United States Code (USC).

> "(8) the term 'information system' means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information;"

The accepted DoD definition of 'Information Technology' is contained within Title 40, USC 1401, Sec. 5002(3), also known as The Clinger-Cohen Act of 1996:

> "(3) Information Technology - (A) The term 'information technology', with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency…
>
> (B) The term 'information technology' includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

(C) Notwithstanding subparagraphs (A) and (B), the term 'information technology' does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract."

Title 40, USC 1401, Sec. 5142 also defines 'National Security Systems':

"(a) DEFINITION - In this subtitle, the term 'national security system' means any telecommunications or information system operated by the United States Government, the function, operation, or use of which--

(1) involves intelligence activities;

(2) involves cryptologic activities related to national security;

(3) involves command and control of military forces;

(4) involves equipment that is an integral part of a weapon or weapons system; or

(5) subject to subsection (b), is critical to the direct fulfillment of military or intelligence missions.

(b) LIMITATION – Subsection (a)(5) does not include a system that is to be used for routine administrative and business applications (e.g., payroll, finance, logistics, personnel management)."

DoD Instruction 5000.2, Change 1, dated January 4, 2000, defines 'weapon system' as:

"A 'weapon system' is an item or set of items that can be used directly by warfighters to carry out combat or combat support missions to include tactical communications systems."

For the initial registration, March 22, 2001, weapon systems should be included at the system level rather than the subsystem level.

Finally, the following definitions for 'Mission Critical Information Technology System' and 'Mission Essential Information Technology System' are now included in DoDI 5000.2, Change 1, dated January 4, 2001:

"E.2.1.12. Mission Critical Information System. A system that meets the definitions of 'information system' and 'national security system' in the Clinger-Cohen Act, the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (Note: The designation of mission critical should be made by a Component Head, a CINC or their designee.) Mission Critical Information Technology System has the same meaning as a Mission Critical Information System.

E.2.1.13. Mission Essential Information System. A system that meets the definition of 'information system' in the Clinger-Cohen Act, that the acquiring Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (Note: The designation of mission essential should be made by a Component Head, a CINC or their designee.)

Mission Essential Information Technology System has the same meaning as a Mission Essential Information System."

Registration

To obtain an account for the DoD IT Registry, users should register on the NIPRNet at https://www.itdb.c3i.osd.mil (or on the SIPRNet at http://207.85.97.11) by completing the on-line application form for new users. Upon verification of identity, new users will be granted access to the DoD IT Registry by the DoD IT Registrar.

DoD Component CIOs are responsible to ensure all MC/ME IT systems are registered and updated on a quarterly basis, as follows:

1) The current DoD IT Registry shall be used to build the consolidated inventory of DoD systems as required by Section 8102(a) of the FY2001 National Defense Appropriation Act and Section 811(a) of the FY 2001 National Defense Authorization Act:

   "…maintain a consolidated inventory of Department of Defense mission critical and mission essential information systems…"

2) Each Component will first validate their existing entries in the DoD IT Registry to determine that their entries are still valid considering the recently published definitions of Mission Critical Information Technology System and Mission Essential Information Technology System from DoDI 5000.2, Change 1, dated January 4, 2001 above.
3) All entries that are not MC/ME IT systems under the new definitions should be removed from the DoD IT Registry. Components will coordinate the deletion of those registry entries with the DoD IT Registrar, who will remove them from the DoD IT Registry.
4) As was done with previous year's registration efforts, each Component CIO will certify by letter to the DoD CIO that their MC/ME IT systems have all been registered. These certification letters are to be provided by March 22, 2001, 2002, and 2003.
5) My POC for the DoD IT Registry is Mr. Gary Evans, (703) 602-0980 extension 137, Gary.Evans@osd.mil.

In last years IT registration, some DoD components did not fill all required data fields (such as ACQ_CATEGORY or FUNC_AREA) for each registered IT system. The data fields in Table 1 of Appendix C will be used for the IT systems registered and certified by March 22, 2001.

Identification of System Interfaces

The complete text of Section 8102 is at Appendix A. Text of Section 811 is contained in Appendix B. Section 811(a) actually contains the language that requires DoD to:

> "…identify interfaces between those systems and other information systems,…"

Once the DoD IT Registry entries are certified by each Component, the resulting list of MC/ME IT systems becomes the official list for which each Component must identify system interfaces.

One additional data field (Yes/No flag) will be added to the DoD IT Registry and used to indicate if the all of the system interfaces for any particular IT System have been identified. Components should start updating the interface data field in the Registry. The DoD goal is to be able to certify next year that all system interfaces have been identified.

A system interface is defined as an exchange of data from one system (the sending system) to another (the receiving system). The data output from the sending system becomes a data input to the receiving system. The exchange need not be a direct electronic connection. It could take place via magnetic tape or via the NIPRNet for example. Interface data will be maintained in electronic format by each Component in a manner prescribed by the Component CIO.

By March 22, 2002, Components will be required to certify that interfaces have been identified for all MC/ME IT systems.

Contingency Plans

Finally, Section 811(a) contains the language which requires DoD to:

> "…develop and maintain contingency plans for responding to a disruption in the operation of any of those information systems…"

Once the DoD IT Registry entries are certified by each Component, and the interfaces are identified for each of those systems, the baseline information is at hand to develop and maintain contingency plans.

A contingency plan in this legislation is narrowly aimed at "responding to a disruption in the operation of those information systems" and is not aimed at a wider definition of performing the business function itself without benefit of automation over a long time period. It is known and expected that most DoD systems have existing contingency plans in place, such as Continuity of Operations Plans (COOPs), which are designed to respond to disruptions in the operation of information systems. There is no requirement to forward contingency plans to the OSD level. These plans rightly belong with the operations staffs who run these systems.

One additional data field (Yes/No flag) will be added to the DoD IT Registry and used to indicate if the contingency plan for the system has been written. Components should start

updating the contingency plan data field in the registry. The DoD goal is to certify next year that contingency plans are in place for all MC/ME IT systems.

By March 22, 2002, Component CIOs will be required to certify that contingency plans are in place for all of their MC/ME IT systems.

Top Secret/Sensitive Compartmented Information (TS/SCI) Systems

TS/SCI MC/ME IT systems are required to be registered. Further guidance will be provided to the DoD community via separate correspondence.

Special Access Programs

The POC for the Special Access Programs registration is LTC Mike Grove at (703) 697-1282 michael.grove@osd.mil. All Special Access Programs will follow the guidance in the DoD Special Access Program Central Office (SAPCO) Director memorandum of March 31, 2000 and should forward their reports through appropriate channels to the following offices:

- DACS-DMP for the Army,
- N-89 for the Navy,
- SAF/AAZ for the Air Force, and
- OUSD (AT&L)/DSP for all others.

New Data Fields and Requirements

The DoD IT Registry IPT is reviewing additional data fields to be added to the DoD IT Registry at this time. Once the data field is approved, the data field will be added for the next quarterly update.

APPENDIX A

The Complete Text of Section 8102, DoD FY 2001 Appropriation Act, PL 106-259 (Signed August 9, 2000) which originated from H.R.4576

Department of Defense Appropriations Act, 2001 (Enrolled Bill (Sent to President))

SEC. 8102. (a) REGISTERING INFORMATION TECHNOLOGY SYSTEMS WITH DOD CHIEF INFORMATION OFFICER- None of the funds appropriated in this Act may be used for a mission critical or mission essential information technology system (including a system funded by the defense working capital fund) that is not registered with the Chief Information Officer of the Department of Defense. A system shall be considered to be registered with that officer upon the furnishing to that officer of notice of the system, together with such information concerning the system as the Secretary of Defense may prescribe. An information technology system shall be considered a mission critical or mission essential information technology system as defined by the Secretary of Defense.

(b) CERTIFICATIONS AS TO COMPLIANCE WITH CLINGER-COHEN ACT- (1) During the current fiscal year, a major automated information system may not receive Milestone I approval, Milestone II approval, or Milestone III approval, or their equivalent, within the Department of Defense until the Chief Information Officer certifies, with respect to that milestone, that the system is being developed in accordance with the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.). The Chief Information Officer may require additional certifications, as appropriate, with respect to any such system.

(2) The Chief Information Officer shall provide the congressional defense committees timely notification of certifications under paragraph (1). Each such notification shall include, at a minimum, the funding baseline and milestone schedule for each system covered by such a certification and confirmation that the following steps have been taken with respect to the system:

(A) Business process reengineering.
(B) An analysis of alternatives.
(C) An economic analysis that includes a calculation of the return on investment.
(D) Performance measures.
(E) An information assurance strategy consistent with the Department's Global Information Grid.

(c) DEFINITIONS- For purposes of this section:

(1) The term 'Chief Information Officer' means the senior official of the Department of Defense designated by the Secretary of Defense pursuant to section 3506 of title 44, United States Code.

(2) The term ‘information technology system’ has the meaning given the term ‘information technology’ in section 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401).

(3) The term ‘major automated information system’ has the meaning given that term in Department of Defense Directive 5000.1.

APPENDIX B

The Complete Text of Section 811 of the DoD FY 2001 Authorization Act (Signed October 30, 2000)

SEC. 811. ACQUISITION AND MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) Responsibility of DOD Chief Information Officer Relating to Mission Critical and Mission Essential Information Technology Systems: Section 2223(a) of title 10, United States Code, is amended--

(1) by striking 'and' at the end of paragraph (3);

(2) by striking the period at the end of paragraph (4) and inserting '; and'; and

(3) by adding at the end the following:

'(5) maintain a consolidated inventory of Department of Defense mission critical and mission essential information systems, identify interfaces between those systems and other information systems, and develop and maintain contingency plans for responding to a disruption in the operation of any of those information systems.'.
(b) Minimum Planning Requirements for the Acquisition of Information Technology Systems: (1) Not later than 60 days after the date of the enactment of this Act, Department of Defense Directive 5000.1 shall be revised to establish minimum planning requirements for the acquisition of information technology systems.
(2) The revised directive required by (1) shall--

(A) include definitions of the terms 'mission critical information system' and 'mission essential information system';

(B) prohibit the award of any contract for the acquisition of a mission critical or mission essential information technology system until--

(i) the system has been registered with the Chief Information Officer of the Department of Defense;

(ii) the Chief Information Officer has received all information on the system that is required under the directive to be provided to that official; and

(iii) the Chief Information Officer has determined that there is in place for the system an appropriate information assurance strategy; and

(C) require that, in the case of each system registered pursuant to subparagraph (B)(i), the information required under subparagraph (B)(ii) to be submitted as part of the registration

shall be updated on not less than a quarterly basis.
(c) Milestone Approval for Major Automated Information Systems: The revised directive required by subsection (b) shall prohibit Milestone I approval, Milestone II approval, or Milestone III approval (or the equivalent) of a major automated information system within the Department of Defense until the Chief Information Officer has determined that--

(1) the system is being developed in accordance with the requirements of division E of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.);

(2) appropriate actions have been taken with respect to the system in the areas of business process reengineering, analysis of alternatives, economic analysis, and performance measures; and

(3) the system has been registered as described in subsection (b)(2)(B).
(d) Notice of Redesignation of Systems: (1) Whenever during fiscal year 2001, 2002, or 2003 the Chief Information Officer designates a system previously designated as a major automated information system to be in a designation category other than a major automated information system, the Chief Information Officer shall notify the congressional defense committees of that designation. The notice shall be provided not later than 30 days after the date of that designation. Any such notice shall include the rationale for the decision to make the designation and a description of the program management oversight that will be implemented for the system so designated.
(2) Not later than 60 days after the date of the enactment of this Act, the Chief Information Officer shall submit to the congressional defense committees a report specifying each information system of the Department of Defense previously designated as a major automated information system that is currently designated in a designation category other than a major automated information system including designation as a 'special interest major technology initiative'. The report shall include for each such system the information specified in the third sentence of paragraph (1).
(e) Annual Implementation Report: (1) The Secretary of Defense shall submit to the congressional defense committees, not later than April 1 of each of fiscal years 2001, 2002, and 2003, a report on the implementation of the requirements of this section during the preceding fiscal year.
(2) The report for a fiscal year under paragraph (1) shall include, at a minimum, for each major automated information system that was approved during such preceding fiscal year under Department of Defense Directive 5000.1 (as revised pursuant to subsection (b)), the following:

(A) The funding baseline.
(B) The milestone schedule.
(C) The actions that have been taken to ensure compliance with the requirements of this section and the directive.
(3) The first report shall include, in addition to the information required by paragraph (2), an explanation of the manner in which the responsible officials within the Department of

Defense have addressed, or intend to address, the following acquisition issues for each major automated information system planned to be acquired after that fiscal year:

(A) Requirements definition.
(B) Presentation of a business case analysis, including an analysis of alternatives and a calculation of return on
investment.
(C) Performance measurement.
(D) Test and evaluation.
(E) Interoperability.
(F) Cost, schedule, and performance baselines.
(G) Information assurance.
(H) Incremental fielding and implementation.
(I) Risk mitigation.
(J) The role of integrated product teams.
(K) Issues arising from implementation of the Command, Control, Communications, Computers, Intelligence,
Surveillance, and Reconnaissance Plan required by Department of Defense Directive 5000.1 and Chairman of the
Joint Chiefs of Staff Instruction 3170.01.
(L) Oversight, including the Chief Information Officer's oversight of decision reviews.
(f) Definitions: In this section:
(1) The term 'Chief Information Officer' means the senior official of the Department of Defense designated by the Secretary of Defense pursuant to section 3506 of title 44, United States Code.
(2) The term 'information technology system' has the meaning given the term 'information technology' in section 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401).
(3) The term 'major automated information system' has the meaning given that term in Department of Defense Directive 5000.1.

APPENDIX C

DoD IT Registry
Field Definitions and Value Tables
Table 1. DoD IT Registry Format

Field Name	Field Size	Field Description
*COMPONENT	25	Executive Agency or DoD Component that owns this MC/ME IT system and is forwarding the data file to the data repository. For acceptable values, see **Table 2** below.
*SYSTEM_ID	20	The distinct System Identification Number or Code used on the Component's database for this MC/ME IT system.
*MISSION_CRITICAL	2	The mission criticality of this IT system. Acceptable values are MC or ME.
SYSTEM_ACRONYM	30	A shortened or commonly used name or abbreviation (upper case) for this MC/ME IT System.
SYSTEM_NAME	100	The full descriptive name for this MC/ME IT system (upper case).
SYSTEM_DESCRIPT	255	A free form text description of the system, its function, and uses.
*ACQ_CATEGORY	3	The acquisition category for this program. For acceptable values, see **Table 3** below.
*FUNC_AREA	50	Relates to the functions under which this particular MC/ME IT system is reported. For acceptable values, see **Table 4** below.
SEC_FUNC_AREA	50	For use if this MC/ME IT system has a secondary function. For acceptable values, see **Table 4** below.
TERC_FUNC_AREA	50	For use if this MC/ME IT system has a tertiary function. For acceptable values, see **Table 4** below.
PM_NAME	50	First and Last name of Program Manager (PM) or POC for this MC/ME IT System
PM_TITLE	10	Rank, Grade, and Title of PM or POC.
PM_ORGANIZATION	50	Organization of PM or POC.
PM_COM_PHONE	18	Commercial phone number of PM or POC.
PM_DSN_PHONE	18	Defense Switched Network phone number of PM or POC.
PM_EMAIL	100	Email address of PM or POC
BIN	6	Insert the Budget Initiative Number if it exists, from the Information Technology Management Application (ITMA) Database.
INTERFACES_IDENTIFIED	3	Indicates if the system interfaces between this MC/ME IT system and other systems have all been identified. Acceptable values are **Yes, No, or NA.**
CONTINGENCY_PLAN	3	Indicates if a contingency plan is in place to account for disruptions in the operations of this system. Acceptable values are **Yes, No, or NA.**
DODREGID	8	Registration identifier. For instructions, see Table 5 below. **Optional field that is not required for March 2001.**

'*****' These fields must be populated with acceptable values or the record will be rejected.

Table 2. Acceptable Values for Component

DoD COMPONENTS	
Army	BMDO
Navy	DARPA
USAF	DCAA
USMC	DeCA
Joint Staff	DFAS
JFCOM	DHRA
CENTCOM	DISA
EUCOM	DLA
PACOM	DSCA
SOCOM	DSS
SOUTHCOM	DTRA
SPACECOM	AFIS
STRATCOM	OASD/HA
TRANSCOM	OSD (ALL)
DoDIG	NORAD
WHS	USFK
DUSD (ES)	DIA
NIMA	NRO
NSA	DCMA
WHCA	

Table 3. Acceptable Values for Acquisition Category

ACQUISITION CATEGORY
I
ID
IC
IA
IAM
IAC
II
IIA
III
IV
NA

Table 4. Acceptable Values for Functional Area

FUNCTIONAL AREAS
Allies
Civilian Personnel
Command and Control
Communications
COMSEC
Economic
Environmental Security
Facilities
Finance
Health
Human Resources
Information Management
Inspector General
Intelligence
Logistics
Military Personnel and Readiness
Nuclear
Nuclear, Chemical, and Biological
Personnel and Readiness
Procurement
Reserve Components
Scientific and Engineering
Space and Weather
Test and Evaluation
Trainers
Weapons
NA

Table 5. Instructions for Registration Identifier

The DODREGID is an 8-character identifier used to uniquely identify systems in the DoD IT Registry. This unique identifier is created by the Components when a system entry is created. The valid characters in the DODREGID are the uppercase letters and the digits 0 thru 9 [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]. The first 2 positions of the 8-character ID are assigned by OSD to each Component in accordance with the table below. The remaining 6-characters are assigned by the Component. The DODEGID must always contain 8 valid characters. This field is optional for the March 2001 registration.

Component	ID Range
AFIS	AA
Army	AB
BMDO	AC
CENTCOM	AD
DARPA	AE
DCAA	AF
DCMA	AG
DeCA	AH
DFAS	AI
DHRA	AJ
DIA	AK
DISA	AL
DLA	AM
DoDIG	AN
DSCA	AO
DSS	AP
DTRA	AQ
DUSD (ES)	AR
EUCOM	AS
JFCOM	AT
Joint Staff	AU
Navy	AV
NIMA	AW
NORAD	AX
NRO	AY
NSA	AZ
OASD/HA	BA
OSD (ALL)	BB
PACOM	BC
SOCOM	BD
SOUTHCOM	BE
SPACECOM	BF

STRATCOM	BG
TRANSCOM	BH
USAF	BI
USFK	BJ
USMC	BK
WHCA	BL
WHS	BM